CLAIMS

WHAT IS CLAIMED IS:

A1. A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system; and

converting to a second basis using a mixed radix system.

A2. The method of claim A1, wherein the ring arithmetic function includes multiplication.

A3. The method of claim A1, wherein the ring arithmetic function includes addition.

A4. The method of claim A1, wherein the ring arithmetic function includes subtraction.

A5. The method of claim A1, wherein the data is encrypted using asymmetric encryption.

A6. The method of claim A1, wherein the data is encrypted using symmetric encryption.

A7. The method of claim A1, further comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

A8. The method of claim A7,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

A9. The method of claim A8, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus C $= S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

A10. The method of claim A1, further comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

A11. The method of claim A10,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

B1. A method of encrypting data comprising the steps of:

choosing a first basis (m_1, m_2, ... mt);

choosing a second basis (m_{t+1}, m_{t+2}, ... m_{2t});

calculating a product $M = m_1 m_2 \ldots m_t$;

calculating a product $W = m_{t+1} m_{t+2} \ldots m_{2t}$; and

calculating a product $ABM^{-1} \bmod p$, wherein the calculating a product $ABM^{-1} \bmod p$ includes:

computing Q mod M in the first basis such that $AB + Qp = RM$ for some integral value R;

converting Q to the second basis, Q mod W; and

computing R in the second basis, R mod W, wherein $R = (AB + Qp)M^{-1} \bmod W$ and $R \bmod p = ABM^{-1} \bmod p$.

B2. The method of claim B1, further comprising converting R to the first basis, R mod M.

B3. The method of claim B2, further comprising:

a second iteration of the method of claim B2; and

wherein R is used as input to the subsequent iteration.

B4. The method of claim B1, wherein the data is encrypted using asymmetric encryption.

B5. The method of claim B1, wherein the data is encrypted using symmetric encryption.

C1. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

C2. The method of claim C1,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

C3. The method of claim C2, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus C $= S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

D1. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

D2. The method of claim D1,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

E1. A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system; and

converting to a second basis using a mixed radix system.

E2. The method of claim E1, wherein the ring arithmetic function includes multiplication.

E3. The method of claim E1, wherein the ring arithmetic function includes addition.

E4. The method of claim E1, wherein the ring arithmetic function includes subtraction.

E5. The method of claim E1, further comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

E6. The method of claim E5,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

E7. The method of claim E6, further comprising

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus C $= S_2$ if $S_3 < 2^w$, and wherein the modulus C $= S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

E8. The method of Claim E7, wherein the method of hashing data comprises a method of cryptographic hashing.

E9. The method of claim E1, further comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

E10. The method of claim E9,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.